VI - profissionalização e caráter perene da atividade, inclusive com conexão com outras áreas internas para proteção integral da Instituição, de seus integrantes e demais ativos;
VII - integração do MPPA com outros órgãos essenciais à atividade de segurança institucional;
VIII - orientação da atividade às ameaças reais ou potenciais à Instituição e a seus integrantes, inclusive no que tange aos efeitos de acidentes naturais;
IX - salvaguardar sempre a Instituição, evitando sua exposição e exploração midiática negativa; e
X - proteção aos direitos fundamentais e respeito aos princípios constitucionais reitores da atividade administrativa.

CAPÍTULO IV
DAS DEFINIÇÓES

Art. 7º A presente política deve se orientar conforme as seguintes definições:
I - Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano ao MPPA;
II - Aplicativos de Comunicação Instantânea ou Mensageria: conjuntos de códigos e instruções compilados, executados ou interpretados por um recurso de Tecnologia da Informação e Comunicação (TIC), armazenados em um dispositivo ou na nuvem, que são usados para troca rápida de mensagens, conteúdos e informações multimídia;
III - Ativo: é qualquer objeto que tenha valor para o MPPA e precisa ser adequadamente protegido;
IV - Ativo Intangível: todo elemento que possui valor para o MPPA e que esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível, a exemplo, mas não se limitando, à reputação, imagem, marca e conhecimento;
V - Autenticidade: garantia de que a informação foi criada, editada ou emitida por quem se disse ter sido, sendo capaz de gerar evidências não repudiáveis em relação ao criador, editor ou emissor.
VI - "Backup": salvaguarda de informações realizada por meio de reprodução e/ou espelhamento de uma base de arquivos com a finalidade de plena capacidade de recuperação em caso de incidente ou necessidade de "restore", ou ainda, constituição de infraestrutura de acionamento imediato em caso de incidente ou necessidade justificada do MPPA;
VII - Colaborador: expressão que compreende membro, servidor, empregado, estagiário, prestador de serviço, terceirizado, fornecedor, menor aprendiz ou qualquer outro indivíduo ou organização que venha a ter relacionamento profissional com o MPPA, direta ou indiretamente;
VIII - Confidencialidade: garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento dos não autorizados;
IX - Disponibilidade: garantia de que as informações e os Recursos de TIC estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso;
X - Dispositivos Móveis: equipamentos de pequena dimensão que têm como características a capacidade de registro, armazenamento ou processamento de informações, possibilidade de estabelecer conexões e interagir com outros sistemas ou redes, além de serem facilmente transportados devido a sua portabilidade, como por exemplo, "pen drive", celular, "smartphone", computadores portáteis, "tablet", equipamento reprodutor de MP3, câmeras de fotografia ou filmagem, ou qualquer dispositivo que permita conexão à Internet ou armazenagem de dados;
XI - Dispositivos Removíveis de Armazenamento de Informação: dispositivos capazes de armazenar informações e possibilitara portabilidade dos dados, como CD, DVD, "pen drive" e discos rígidos (HD) externos;
XII - Gestor da Informação: responsável pela atribuição do nível de classificação que a informação demanda, e pela definição do método como é gerada, armazenada, transmitida, descartada, entre outros processos;
XIII - Homologação: processo de avaliação e aprovação técnica de recursos de TIC para serem utilizados dentro do ambiente do MPPA;
XIV - Identidade Digital: é a identificação do colaborador em ambientes lógicos, sendo composta por seu nome de usuário (login) e senha ou por outros mecanismos de identificação e autenticação como crachá magnético, certificado digital, "token" e biometria;
XV - Incidente de Segurança da Informação: ocorrência identificada de um estado de sistema, dados informações, serviço ou rede que indica possível violação à Política de Segurança da Informação ou normas complementares, falha de controles ou situação previamente desconhecida e que possa ser relevante a segurança da informação;
XVI - Informação: conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato;
XVII - Integridade: garantia de que as informações estejam fidedignas em relação à última alteração desejada durante o seu ciclo de vida;
XVIII - Internet: rede mundial de computadores interconectada pelo protocolo TCP/IP, cuja infraestrutura tem caráter aberto e colaborativo, acessível por meio de dispositivos com conexão e autorizações suficientes e que permite obter informação de qualquer outro dispositivo que também esteja conectado à rede, desde que configurado adequadamente;
XIX - Legalidade: garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do ordenamento jurídico em vigor;
XX - Quebra de Segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação nos recursos de TIC do MPPA;
XXI - Programas Maliciosos: códigos que têm como objetivo ou consequência comprometer a segurança do dispositivo que o executa, ou da integridade, confidencialidade ou disponibilidade de seus dados, ou, ainda, gerar perturbações ou interrupções em sua utilização;
XXII - Recursos de Tecnologia da Informação e Comunicação (Recursos de TIC): todos os recursos físicos e lógicos utilizados para criar, armazenar, manusear, transportar, compartilhar e descartar a informação. Entre os tipos de recursos, destacam-se computadores de mesa ou portáteis, "smartphones", "tablets", "pen drives", discos externos, mídias, impressoras, "scanners" e outros. Sempre que mencionados de forma a não identificar seu possuidor ou proprietário, os recursos de TIC compreenderão tanto os pertencentes ao MPPA quanto aos particulares em proveito institucional. Caso contrário, haverá declinação de posse ou propriedade no próprio texto;
XXIII - Repositórios Digitais ("Cyberlockers"): plataformas de armazenamento na Internet, a exemplo, mas não se limitando, ao "Google Drive", "OneDrive", "Dropbox", "iCIoud", "Box", "SugarSync", "Slideshare" e "Scribd";
XXIV - Risco: combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos;
XXV - Segurança da Informação: preservação da confidencialidade, integridade, disponibilidade, legalidade e autenticidade da informação. Visa proteger a informação e os recursos de TIC que as contêm dos diversos tipos de ameaças para garantir a continuidade da finalidade institucional, minimizar os danos às suas atividades, além de maximizar o retorno dos investimentos e de novas oportunidades de transação;
XXVI - Tentativa de Burla: atos que busquem violar as diretrizes estabelecidas nos documentos normativos do MPPA e sejam frustrados por erro durante o planejamento ou durante sua execução; e
XXVII - Violação: qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos do MPPA.

CAPÍTULO V
DAS MEDIDAS DE SEGURANÇA INSTITUCIONAL

Art. 8º A segurança institucional compreende o conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar ações de qualquer natureza que constituam ameaça à salvaguarda da Instituição e de seus integrantes, inclusive no que tange à sua imagem e reputação.
§ 1º As medidas de segurança institucional compreendem a segurança orgânica e a segurança ativa.
§ 2º A segurança orgânica e composta pelos seguintes grupos de medidas:
I - segurança de pessoas e recursos humanos;
II - segurança do material;
III - segurança das áreas e instalações; e
IV - segurança da informação e de tecnologia da informação.
§ 3º A segurança ativa compreende ações de caráter proativo e englobam, no âmbito do Ministério Público, medidas de contrassabotagem, contraespionagem, contra crime organizado e contrapropaganda.

Seção I
Da Segurança de Pessoas e Recursos Humanos

Art. 9º A segurança de pessoas e recursos humanos compreende o conjunto de medidas voltadas a proteger a integridade física de membros, de servidores e de seus respectivos familiares em face dos riscos, concretos ou potenciais, decorrentes do desempenho das funções institucionais.
§ 1º A segurança de pessoas e recursos humanos, entre outras ações, abrange as operações de segurança, atividades planejadas e coordenadas, com emprego de pessoal, material, armamento e equipamento especializado e subsidiadas por conhecimento de inteligência a respeito da situação.
§ 2º A segurança de pessoas e de recursos humanos poderá ser realizada por servidores do Ministério Público com atribuições pertinentes e/ou mediante cooperação ou solicitação aos respectivos órgãos de segurança pública estaduais ou federais, por outros servidores, policiais, militares e/ou por empresas especializadas.
§ 3º Abrange ainda como segurança de pessoas:
I - pessoas que ingressem ou transitem nas instalações do MPPA; e
II - participantes e colaboradores em eventos ou atividades promovidas pelo MPPA.

Seção II
Da Segurança de Material

Art. 10. A segurança de material compreende o conjunto de medidas voltadas a proteger o patrimônio físico, bens móveis e imóveis, pertencente ao Ministério Público ou sob o uso da Instituição.
§ 1º O material compreende o patrimônio físico do MPPA, constituído por bens móveis e imóveis, que permite o adequado funcionamento de uma Unidade.
§ 2º As medidas de guarda e proteção do material devem observar as condições técnicas e os procedimentos de segurança e manutenção específicos do material.

Seção III
Da Segurança de Áreas e Instalações

Art. 11. A segurança de áreas e instalações compreende o conjunto de medidas voltadas a proteger o espaço físico sob responsabilidade do Ministério Público ou onde se realizam atividades de interesse da Instituição, com a finalidade de salvaguardá-las.
§ 1º A segurança de áreas e instalações engloba as seguintes atividades, dentre outras:
I - demarcação, classificação e sinalização das áreas, nos termos da legislação pertinente;
II - controle de acessos e controle do fluxo de pessoas, inclusive com uso obrigatório de crachás para todos os integrantes da Instituição;
III - detecção de intrusão e monitoramento de alarme;
IV - implantação de barreiras perimétricas;
V - estabelecimento de linhas de proteção;
VI - sistema de vigilância pessoal;
VII - proteção de cabeamentos e quadros de toda espécie;
VIII - proteção de sistemas de energia, água, gás e ar-condicionado;
IX - prevenção e combate a incêndio;
X - instalação de aparelho detector de metais, aos quais devem se sub-